2024-25 DCIG TOP 5
2PB+ CYBER SECURE BACKUP TARGETS // US EDITION

By DCIG Principal Data Protection Analyst, Jerome M Wendt

2PB+ Cyber Secure Backup Targets // US Edition

Table of Contents

2PB+ Cyber Secure Backup Targets // US Edition

SOLUTIONS EVALUATED

1. Dell PowerProtect DD9400
2. Dell PowerProtect DD9900
3. ExaGrid EX27
4. ExaGrid EX36
5. ExaGrid EX54
6. ExaGrid EX84
7. ExaGrid EX189
8. Infinidat InfiniBox F6320
9. Infinidat InfiniGuard 83420
10. InforTrend EonStor CS 4000
11. InforTrend EonStor GS 4000
12. iXsystems TrueNAS M40
13. iXsystems TrueNAS M50
14. iXsystems TrueNAS M60
15. iXsystems TrueNAS R50
16. Nexsan Unity NV10000
17. Pure Storage FlashArray//E
18. Pure Storage FlashBlade//E
19. Pure Storage FlashArray//C90
20. Qnap TS-h2287XU-RP
21. Quantum DXi9000
22. Quantum DXi9100
23. RackTop Systems BrickStor SP BSND41025
24. RackTop Systems BrickStor SP BSND41125
25. VAST Data Platform

CYBER SECURE BACKUP TARGET FEATURES EVALUATED

- API/network protocols supported.
- Data protection.
- Hardware configuration.
- Management.
- Technical support.

Cyber Security Becomes Core Backup Target Feature

Enterprises have historically measured backup targets based on how well they minimally deliver on the following three features:

- Backup throughput speeds.
- Data reduction.
- Economical storage.

Ransomware threats and attacks have forced enterprises to add at least one more core feature to this list: cyber security.

Enterprises and managed service and technology providers now regularly report that many ransomware stains routinely target their backup infrastructures. Some ransomware strains even start their attacks by seeking to compromise or disable backup targets. This do so in one or more of the following ways:

- Compromise or obtain administrative logins to these systems.
- Delete backups residing on them.
- Encrypt backups residing on them.
- Exfiltrate, or copy, backups from the system to the hacker's site.

The Incentive for Hackers to First Attack Backup Targets

Ransomware first attacking backup targets hinders an enterprise's ability to recover from an attack. Having compromised the backup target in any of these ways, the ransomware then turns to attacking production IT data and systems. If it then succeeds in these attacks in production, enterprises may find themselves without any restoration or recovery options.

Further adding to the danger of ransomware attacks, 90 percent of these attacks exfiltrate data.[1] Hackers may use exfiltrated data as another means to extract a ransom. Alternatively, hackers may sell the data to third parties, release it publicly, or take all these actions. Further complicating matters, enterprises may lack clarity into how hackers accessed their IT infrastructure and the data they stole.[2]

Hackers may also attempt to obtain a backup target's administrative logins and passwords. If they log into the backup target with administrative permissions, a hacker may perform any number of nefarious activities. These can range from deleting backups to copying backups offsite to changing file permissions and backup retention periods.

Finally, even should the backup target repel a ransomware attack, the ransomware may still compromise production systems and data. In this common scenario, enterprises may need the backup target to assume additional roles. These can include performing instant restores and hosting recoveries even as the solution continues functioning as a backup target.

Repelling these different attack types and assuming broader recovery capabilities demands that enterprises choose cyber secure backup targets. These backup targets still deliver on the core three features that enterprises expect backup targets to possess. However, cyber security features have become prerequisites for enterprises seeking to protect their backups and facilitate fast restores and recoveries.

1. https://www.blackfog.com/the-state-of-ransomware-in-2023/. Referenced 1/8/2024.
2. Ibid.

2PB+ Cyber Secure Backup Targets // US Edition

This report focuses on cyber secure backup targets that offer file protocol support in the US market.

The State of Cyber Secure Backup Targets

Only recently have storage providers, as a group, begun positioning their network attached storage (NAS) solutions as backup targets. Prior to that, few storage providers formally marketed their NAS systems as backup targets. While NAS systems could serve in this role, providers downplayed this functionality.

Today, few providers exhibit any concerns about their NAS solutions being used as backup targets. More than 20 different storage providers promote more than 100 production storage systems on their respective websites as backup targets.

While many of these storage systems support multiple storage protocols, this report focuses on solutions that offer file protocol support. These support either the Network File System (NFS), the Common Internet File System (CIFS), or both. These NAS solutions provide the following benefits for backup that enterprises frequently want:

- Backup software can easily discover and utilize these solutions as backup targets.
- Client-side software available to accelerate backup throughput.
- Facilitate fast application, and data, restores.
- Fast, easy deployment, setup, and management in enterprise backup infrastructures.
- Readily recognized as a storage target by all commonly used operating systems.
- Utilize standard, cost-effective Ethernet for network connectivity.

Available Cyber Backup Target Cyber Security Features

All the backup targets evaluated offer cyber secure capabilities, though the availability, breadth, and implementation of these features vary.

Data Immutability

Data immutability, or storing data in an unchangeable format, represents one feature nearly every backup target supports. When enabled, this feature prevents ransomware attacks from either deleting or encrypting backups stored on the backup target.

Encryption

Encryption represents another backup target feature that has seen an uptick in adoption. Many backup targets have offered at-rest encryption for years. However, few enterprises used it due to the overhead it incurs while encrypting or decrypting backups.

This corporate mindset toward using at-rest encryption has since changed. Many ransomware strains attempt to exfiltrate data as part of their attack. Admittedly, encrypting backups does not prevent ransomware from exfiltrating them outside of the enterprise. However, hackers will find it almost impossible to decrypt and read any encrypted backups they obtain.

Multi-factor Authentication

Using multi-factor authentication (MFA) to log into a cyber secure backup target represents perhaps the most significant enhancement in recent years. Implementing MFA helps ensure only the appropriate administrators access and manage the backup target.

Some backup targets even require a second administrator to authenticate before it allows certain configuration changes. These may include tasks such as changing folder permissions or deleting data, among others.

High Availability

High availability (HA) also appears as a cyber security enhancement with more backup targets offering highly available controller configurations. Enterprises may not normally view HA in the context of cyber security. However, HA has become relevant due to the role that backup targets play in helping enterprises recover from a ransomware attack.

HA has become relevant due to the role that backup targets play in helping enterprises recover from a ransomware attack.

During restores and recoveries, backup targets may have to perform the following tasks, which include:

- Scanning backups to be used for restores and recoveries for the presence of ransomware.
- Providing fast response times for instant restores.
- Hosting recovered applications and/or data.
- Continuing to serve as a backup target for those parts of the enterprise unaffected by ransomware and still operating normally.
- Retrieving backups from the cloud or offsite locations.

Using backup targets that offer HA better equips them to simultaneously perform some or all these tasks. They give enterprises the extra raw resources (computing, memory, networking, and storage) that they need at these times.

Artificial intelligence

Artificial intelligence (AI) has yet to make significant inroads as a cyber secure feature on most backup targets. This slow adoption of AI in backup targets somewhat stems from other trends already in play.

For instance, enterprise backup software has often implemented AI to detect ransomware in backups. This development has somewhat negated the need for backup targets to include AI that detects ransomware.

Rather, enterprises will primarily find AI in backup targets in its first iteration, machine learning (ML). Currently backup targets may use ML for improved technical support and performing proactive maintenance on their systems. DCIG anticipates through their use of ML to perform these tasks that backup targets will soon offer more sophisticated AI functionality.

The 2PB+ Cyber Secure Backup Target Dividing Line

All 100+ evaluated backup targets that DCIG evaluated do not necessarily compete against one another. Some offer only block (FC and iSCSI) interfaces. Others offer only NAS (CIFS and NFS) interfaces. Still others offer only object (S3) interfaces.

Additionally, some support various combinations of these storage protocols. Some offer unified storage (block and file.) Some support universal storage (block, file, and object.) Still others provide file and object storage.

DCIG opted to solely focus this report on cyber secure backup targets that supported NAS interfaces. While these backup targets may also offer block and/or object interfaces, DCIG only examined their NAS capabilities.

Backup targets using file protocols offer the greatest flexibility when it comes to ease of management, deployment, and backup operations. However, these same characteristics tend to make them more vulnerable to ransomware attacks.

Continued

2PB+ Cyber Secure Backup Targets // US Edition

Ransomware increasingly seeks out and discovers file shares presented by backup targets on enterprise networks.

Ransomware increasingly seeks out and discovers file shares presented by backup targets on enterprise networks. Once discovered, ransomware may attempt to exfiltrate, encrypt, and/or delete backups on these file shares. It may even try to access the backup target itself and gain control of it. These factors contribute to the need for enterprises to select backup targets that offer cyber security features.

Over 90 percent of the 100+ backup targets evaluated by DCIG offered a file system interface. DCIG then eliminated those NAS systems not positioned as backup targets or lacking appropriate cyber security features. Of those backup targets remaining, two petabytes (PB) of raw storage capacity emerged as a natural dividing line between them.

DCIG did view the remaining cyber secure backup targets with NAS as solutions appropriate for enterprises. However, the 2PB+ and sub-2PB system dividing line better reflected which backup targets typically compete against one another.

Common Features Across All 2PB+ Cyber Secure Backup Targets

DCIG evaluated over 100 different backup targets of which 25 met DCIG's criteria for 2PB+ cyber secure backup target for the US Edition of this report. Across these 25 backup targets, DCIG evaluated over 170 features on each one. Despite all these solutions scaling to 2PB or higher, enterprises may only safely assume that each one minimally possesses the following features:

1. ***Four (4) Ethernet ports.*** Since each backup target supports file networking protocols, enterprises would expect they support Ethernet connectivity. Further, enterprises might expect each solution to offer numerous Ethernet ports due to the number of petabytes supported. Yet enterprises may only safely assume the availability of four Ethernet ports on any of these systems. However, over 85 percent scaled to offer at least eight ports.
2. ***Can fit 100 terabytes in every rack unit***. Data center floor space remains some of the most expensive real estate in the world. This often makes optimizing every square inch of available space an imperative. Cyber secure backup targets do their part. Each one can hold no less than 100 terabytes per rack unit (TB/RU). Further, over 85 percent of these backup targets can achieve up to 250 TB/RU.
3. ***Compression.*** Due to more storage systems repositioning themselves as backup targets, enterprises must verify their data reduction capabilities. With respect to this functionality, enterprises may now only assume that all these backup targets offer compression. If they need the solution to deliver deduplication, they should check further. Only slightly more than 70 percent offer deduplication as a core or optional feature.
4. ***NFSv3/SMBv2.*** As a report that focuses on backup targets that offer file protocol support, one may assume they support NFSv3/SMBv2. That assumption would be correct. However, enterprises should not assume these backup targets support all versions of these two file protocols. SMBv3 represents the next most widely supported protocol across these backups targets as nearly 90 percent support it. Enterprises should also verify if the backup target supports and enables SMBv1 by default, as about 50 percent do. If enabled and using SMBv1 on the backup target, this could present an internal cyber security risk.

5. ***Active Directory (AD) and Lightweight Directory Access Protocol (LDAP).*** Storage systems of any type integrating with and supporting AD and LDAP were once more the exception than the rule. No more. The threat of ransomware has led to more storage providers implementing better forms of identity management on their storage systems. As it pertains to these 2PB+ cyber secure backup targets, all now support AD and LDAP.
6. ***Email alerts, notifications, and technical support.*** 2PB+ cyber secure backup targets use at least eight and possibly more means to send out alerts and warnings. However, email represents the only alert and notification feature that enterprises may assume every backup target supports. This even extends to technical support. Enterprises cannot simply assume that because a backup target scales over 2PB that it offers other means of technical support. They can only assume that it offers email technical support.

The threat of ransomware has led to more storage providers implementing better forms of identity management on their storage systems.

Similarities between the TOP 5 2PB+ Cyber Secure Backup Targets

In addition to supporting all the features listed above, each of the TOP 5 2PB+ cyber secure backup targets also support the following additional features. These include:

- ***Support at least two controllers.*** Simply because a backup target scales out to support 2PB+ of storage capacity does not mean it offers HA. However, each of the TOP 5 2PB+ cyber secure backup targets offer at least two controllers to provide some form of HA.
- ***Scale to at least 40 CPU cores.*** Having multiple CPU cores on the backup target often directly impacts its performance during backups and restores. Each of these backup targets scales to at least 40 CPU cores in its largest configuration.
- ***Non-disruptive storage controller replacement.*** HA on backup targets has emerged as a feature that helps enterprises create a more cyber secure, resilient environment. Each of these TOP 5 cyber secure backup targets offer the option to perform non-disruptive storage controller replacements.
- ***SMBv3.*** Enterprises remain hyper concerned about all data in their environment whether at-rest or in-transit. Sending or restoring backups using SMBv3 provides an extra level of security as it offers end-to-end encryption. Each TOP 5 2PB+ cyber secure backup target supports this file networking protocol.
- ***Asynchronous replication.*** Copying backups stored on the backup target to another backup target on-site or offsite provides still more data protection. Each of these TOP 5 backup targets offer asynchronous replication to accomplish this task.
- ***24x7x365 technical support with 1 hour or less response time.*** Enterprises need to have complete confidence that they can reach technical support at any time day or night. Each TOP 5 backup target provider offers this high level of technical support.
- ***Remote monitoring.*** More enterprises do not want to call technical support. They want the provider to tell them their backup target has an issue before it impacts backup or restore operations. Each of these TOP 5 solutions offer remote monitoring to help diagnose and troubleshoot issues on the backup target before it escalates.

Differences between the TOP 5 2PB+ Cyber Secure Backup Targets

The TOP 5 cyber secure backup targets also differ in how they implement specific features that they offer. These differences appear in core features such as backup data optimization network protocols, data encryption, data immutability, and HA. While enterprises may expect backup targets to support these functions, and they largely do, they do also implement them differently. Consider:

Differences in the TOP 5 backup targets appear in core features such as backup data optimization network protocols, data encryption, data immutability, and HA.

- ***Backup data optimization network protocols.*** Many enterprises have become accustomed to using one or more of the available backup data optimization network protocols.

  These protocols, often supplied by backup software providers, may compress and deduplicate backups before sending them to the backup target. Alternatively, or additionally, they may facilitate sending multiple backup jobs at the same time. They may also modify file network protocols so they can send larger packets of data.

  For any of these protocols to work, the backup target often must communicate with the backup software. The backup software will let the backup target know it plans to transmit and retrieve the backup data using this protocol. These protocols can significantly reduce backup traffic over the network while also expediting backups and recoveries.

  The level of support that cyber secure backup targets offer for backup data optimization network protocols varies significantly. Some backup target providers support multiple data optimization network protocols available from numerous backup software providers. In lieu of supporting backup software's optimization software, some backup target providers now offer their own.

- ***Data encryption.*** Encrypting backups stored on the backup target represents another feature that gets used more frequently by enterprises. While each TOP 5 backup target supports it, they may implement it in one of two ways. The software on their array may encrypt the data. Alternatively, they may use internal disk drives that do the encryption. If the backup target uses self-encrypting drives, they may need to order that feature when they acquire the backup target.

- ***Data immutability.*** Every TOP 5 backup target supports data immutability in some format. This feature has particularly come into focus as ransomware attacks often attempt to delete or encrypt backups on backup targets. Storing backups in an immutable data format prevents ransomware from making any changes to the backups.

  Each of the TOP 5 backup targets offers the option to store data in an immutable format. However, they again may implement this feature differently. Some use immutable object storage. Some provide a write once, read many (WORM). Some offer both options. Each offers the option to connect to either cloud storage or another device that can store data in an immutable format.

- ***Storage controller configurations.*** Every TOP 5 cyber secure backup target offers at least two storage controllers in an HA configuration. However, enterprises will find that they implement them differently. Enterprises will find at least six different HA controller configurations available across these TOP 5 backup targets. They include Active-Active, Active-Standby, Dual Active, Federated, Mesh Active, and Scale-out architectures.

  While each storage controller configuration provides HA, benefits and drawbacks exist with each one. For instance, the Active-Active, Active-Standby, and Dual Active architectures all represent established storage controller architectures. They facilitate adding, or scaling up, storage capacity. However, they provide limited or no options to add more CPUs, networking ports, or memory to the two controllers. Enterprises may also need to replace the backup target at the end of its life.

Mesh Active and Scale-out architectures provide more flexibility for enterprises to incrementally add computing, memory, networking ports and storage. In this way enterprises may scale out their backup target as they need. Further, scale-out architectures often facilitate updates of specific nodes without needing to replace the entire backup target. However, enterprises may find that adding more storage capacity also requires they add more computing, memory, and networking ports. In some cases, they may not need those extra resources.

TOP 5 Cyber Secure Backup Target Solution Profiles

Each of the following TOP 5 cyber secure backup target solution profiles highlights at least three ways each one differentiates itself. These differentiators represent some of the best methods that cyber secure backup targets offer to back up, restore, and/or secure data stored on them. Within each solution, enterprises may find specific features that may better meet their specific needs.

ExaGrid EX189

To help quickly resolve any technical backup issues, ExaGrid assigns a level 2 senior support engineer to each customer account.

ExaGrid distinguishes itself as the only scale-out backup target to achieve a TOP 5 ranking. Scaling out to 32 appliances, the EX189 offers nearly 14PB of raw capacity (~12PB usable) in its largest configuration. It can take in over 6PB in a full backup into a single system.

Its scale-out architecture helps organizations minimize or eliminate the need for enterprises to perform forklift upgrades. Enterprises may also mix and match any age or size appliance of ExaGrid's seven different Tiered Backup Storage models in the same scale-out system. This includes older and newer models so enterprises can seamlessly upgrade and deploy only the storage that they need.

Other features that the ExaGrid EX189 offers that further help differentiate it from other TOP 5 2PB+ cyber secure backup targets include:

- Concurrently utilizes multiple features for backup acceleration. ExaGrid represents one of the few, if not the only provider, that only uses HDDs in its backup targets. To deliver faster backup performance than many SSD-based targets, it minimally uses the following three different techniques:
  1. It optimizes its file system for ingesting large file backup jobs.
  2. Uses job concurrency for parallel backups including integrations with the backup application for front-end load balancing.
  3. It offers a disk-cache Landing Zone so backups complete uninterrupted. Its global deduplication only begins after backup writes complete.

- ***Creates a tiered air gap with a delayed delete policy.*** ExaGrid's need to expose the Landing Zone on its systems does make that feature susceptible to ransomware attacks. ExaGrid addresses this concern by offering two other features.

  First, as backup writes complete, ExaGrid immediately copies, deduplicates, and stores data on a non-network facing, air-gapped Repository Tier. Stored in an immutable format, ransomware can then neither access nor change data stored on this tier.

  Second, it offered a configurable delayed delete policy. Backup targets themselves have become susceptible to ransomware attacks with bad actors attempting to log into devices. Implementing the delayed delete policy prevents backups from being deleted even should a hacker take control of an ExaGrid system. Any commands issued to delete data must wait the time specified in the delayed delete policy before a deletion occurs.

- ***Assigns level 2 senior support engineers to each customer account.*** Backup challenges inevitably emerge in every enterprise. To help quickly resolve them, ExaGrid assigns a level 2 senior support engineer to each customer account. This helps engineers become familiar with the customer's backup environment and its history. Support calls placed to ExaGrid then immediately get routed to their assigned engineer who are located around the world.

Infinidat InfiniBox/InfiniGuard

The InfiniSafe feature represents Infinidat's most distinguishing feature set when compared to other cyber secure backup targets.

The complementary Infinidat InfiniBox F6320 and InfiniGuard B4320 cyber secure backup targets meet competing enterprise backup requirements. Both backup targets utilize the same underlying operating system (InfuzeOS) that facilitates fast backups. However, each model includes specific features to address the competing backup and recovery requirements that enterprises may have.

Each enterprise's requirements for how they manage backups and for facilitating fast recoveries will influence their choice between these two Infinidat systems. Enterprises that need a backup target that maximizes available storage capacity should choose the InfiniGuard B4320. This model scales to over 50PBs of storage capacity, offers data deduplication, and uses an InfiniBox as its back-end storage. Those enterprises that need the backup target to host application and data recoveries should give preference to the InfiniBox F6320.

Other features that the InfiniBox F6320 and the InfiniGuard B4320 offer that further help differentiate them from other 2PB+ cyber secure backup targets include:

- ***Built-in InfiniSafe cyber storage technology.*** The InfiniSafe feature represents, perhaps, Infinidat's most distinguishing feature set when compared to other cyber secure backup targets. Included as a core feature on both the InfiniBox and InfiniGuard, InfiniSafe offers key cyber security features that enterprises need today.

  These include immutable snapshots, logical air-gapped data protection, a fenced forensic network, and near-instantaneous recoveries. Infinidat guarantees recoveries in 20 minutes or less for the InfiniGuard B4320 and under one minute for the InfiniBox F6320, regardless of the dataset size.

  Its fenced forensic network specifically stands out among available backup targets. Enterprises may validate backups during recoveries in a private network environment. This helps to ensure recovered backups are ransomware-free so enterprises may safely use the data in production.

- ***Both systems offer high availability with redundant storage hardware.*** The two Infinidat solutions illustrate why highly available backup targets have become a necessity for enterprises. In addition to continually servicing backups, backup targets may also need to facilitate fast restores and perform forensic analysis.

  The Infinidat InfiniBox and InfiniGuard facilitate both of those activities with the InfiniBox optimized for hosting recoveries. Infinidat delivers these high levels of availability and performance. Its storage architecture inherently provides a triple-active redundant architecture. The triple-active architecture ensures that the critical hardware and software components of each system have at least two redundancies. Further, its InfiniRAID technology maintains data integrity beyond normal RAID limitations.

- ***100 percent system availability guarantee.*** Many providers of high-end storage systems jockey for position as to how many "nines" of availability their solution provides. Infinidat minimizes the need for enterprises to have to make calculations for how much downtime they might expect annually. Rather, it provides a 100 percent system availability guarantee specifically for its InfiniBox systems.

The durability of Nexsan's storage systems has become well-documented in the storage industry as they exemplify the "set-it-and-forget-it" tagline.

Nexsan Unity™ NV10000

Having just celebrated its 25th year of providing storage solutions, Nexsan differentiates itself from competitors by providing cost-effective, reliable storage. The durability of its storage systems has also become well-documented in the storage industry as they exemplify the "set-it-and-forget-it" tagline.

The Unity NV10000 represents one of Nexsan's four lines of storage systems. The Unity NV10000 offers a unified storage interface (sometimes referred to as universal storage) with support for block, file, and object storage network protocols.

As a cyber secure backup target, enterprises often utilize the Unity NV10000's NAS interface. However, they may access and use its other storage network protocols at any time since Nexsan offers all-inclusive software licensing.

Other features that the Nexsan Unity NV10000 offers that further help differentiate it from other 2PB+ cyber secure backup targets include:

- ***Highest terabytes per rack unit (TB/RU) of any 2PB+ cyber secure backup target.*** Every enterprise knows how much their data center space costs. The Nexsan Unity NV10000 separates itself from all competitors by effectively utilizing available rack space. When fully populated, it achieves nearly 10 petabytes per RU. Nexsan specifically engineers the Unity NV10000 to account for HDD vibrations. This minimizes HDD failures and extends the life of the HDDs. This results in long life spans (5+ years) for its Unity systems that consume minimal data center floor space.
- ***Offers an immutable, unbreakable backup solution.*** The Unity NV10000 supports block, file, and object storage protocols that respectively offer immutable block and file snapshots and object lock. These features protect enterprise backups and position enterprises to quickly recover. However, some enterprises want even higher levels of protection from ransomware as part of their backup process.

  To accommodate these emerging enterprise demands, Nexsan offers an immutable, unbreakable backup solution. This solution combines the Unity NV10000 with Nexsan's separate Assureon® Active Data Vault.

  In this configuration, enterprises may tier backups off the Unity NV10000 to Assureon to obtain additional data protection features. These features include data integrity checks, more restricted access controls, and self-healing. Further, enterprises may implement Assureon in the cloud, on-premises, or as part of a hybrid cloud configuration.
- ***FASTier™ cache and dual-active controllers for accelerated backups and restores.*** Every enterprise wants to protect its backups from ransomware, but they still must quickly complete backups and restores. To facilitate these activities, the Nexsan Unity NV10000 offers dual-active controllers and a FASTier cache with SSDs. These features work in conjunction with one another to offer high availability, improved processing, and read-and-write caching.

RackTop Systems BrickStor Security Platform

RackTop Systems as a company was founded in 2010 by veterans of the U.S. Intelligence Community. Its background in cyber intelligence and security led to the company embracing enhanced data security since its inception.

RackTop Systems early-on identified the potential threats to backups that cyber security attacks posed. While other backup targets have only more recently begun implementing

The BrickStor Security Platform operates on the premise that no one should be granted implicit trust, not even "approved" employees, contractors, and support personnel.

cyber security features, RackTop has offered them for years. These features specifically show up in how RackTop is at the forefront in utilizing AI to counter ransomware attacks. Consider:

- ***Utilizes a data-centric zero trust architecture.*** The BrickStor Security Platform (SP) operates on the premise that no one should be granted implicit trust, not even "approved" employees, contractors, and support personnel. Using this data-centric zero trust architecture, it utilizes AI to actively defend the data stored on it. It constantly monitors for, and guards against, unusual data access, data deletion, ransomware, insider threats, and excessive file access.

  Taking this approach, BrickStor SP can immediately alert security and infrastructure teams about suspicious behavior. It can also block suspicious user accounts and IP addresses from accessing further data.

- ***Facilitates non-disruptive restores and recoveries from ransomware attacks.*** When a BrickStor SP detects a ransomware attack, it automatically takes action. It begins by immediately generating an incident report. It then blocks suspicious activities and users though it permits non-offending users and applications to continue their operations. Should ransomware successfully delete or encrypt any files, it identifies affected files. It then immediately restores affected files from its immutable snapshots to return the BrickStor SP to full operation.

- ***Performs real time and historical user activity monitoring and analysis.*** The audit log captures extensive details about user activity. This includes the user's identity, source IP address, file operation, protocols used, operation size, and full file path.

  Enterprises may then monitor and analyze this user behavior activity in two way. They may analyze and investigate it within BrickStor SP's user interface. Alternatively, they may have the logs automatically forwarded to a SIEM or anomaly detection engine.

VAST Data Platform

VAST represents one of the few cyber secure backup targets to exclusively use an all-flash architecture.

The VAST Data Platform distinguishes itself by giving enterprises the flexibility to scale either its compute or storage resources independently. To accomplish this, VAST uses a disaggregated and shared-everything architecture (DASE). This design facilitates enterprises adding only the resources that they need as they need them.

VAST also represents one of the few cyber secure backup targets to exclusively use an all-flash architecture. Its architecture uses storage class memory (SCM) as a high performance write buffer and global metadata store. It combines that with dense, low-cost flash (currently quad-level cell (QLC)) which it uses to store backups.

Cyber secure features that the VAST Data Platform offers that help differentiate it from other TOP 5 2PB+ cyber secure backup targets include:

- ***Minimal to no performance backup or recovery penalties despite using data reduction.*** Backup targets often use data reduction technologies such as compression and deduplication to minimize storage costs. However, using these technologies often incurs performance penalties during both backups and restores.

  VAST's DASE architecture coupled with its use of flash minimizes or eliminates the normal performance penalties associated with data reduction. VAST stores all hash tables and data reduction metadata in its SCM layer. It then stores all compressed and deduplicated blocks on its QLC flash. This combination provides high levels of both data reduction and performance while minimizing flash's cost.[3]

3. https://vastdata.com/blog/similarity-reduction-report-from-the-field. Referenced 1/27/2024.

- ***Can instantly recover a VM.*** The VAST Data Platform is a universal, as opposed to a purpose-built, storage system. While it can function as a backup target, it also provides production-level performance so it can host recoveries. Further, VAST compresses and deduplicates ***all*** data stored on its system using its Similarity Reduction algorithm. This architecture lends itself well to performing instant recoveries that may literally instantly occur. Should an enterprise need to restore a VM, it can instantly recover a backed up VM from deduplicated data.
- ***"Quick Clean Room" feature.*** Anytime a ransomware attack occurs, enterprises must always assume a worst-case scenario when performing restores. Among these assumptions, enterprises should start with the assumption that ransomware may reside in the backups they use for restores.

  To help enterprises account for this possibility, the VAST Data Platform offers its Quick Clean Room feature. This feature logically and physically isolates connectivity to the platform's backup data. An enterprise may restore data into this isolated location and test it for ransomware before restoring data into production.

2PB+ Cyber Secure Backup Target Inclusion Criteria

- Available in the US.
- Offers cyber security features to protect itself and data stored on it.
- Scales to at least two petabytes of raw storage capacity.
- Ships as a physical appliance.
- Shipping and available by January 1, 2024.
- Sufficient information available for DCIG to make an informed, defensible decision.

DCIG Disclosures

Providers of some of the 2PB+ cyber secure backup targets covered in this DCIG TOP 5 report are or have been DCIG clients. This is not to imply that their solution was given preferential treatment in this report. In that vein, keep the following points in mind when considering the information contained in this TOP 5 report:

- No provider paid DCIG a fee to research this topic or arrive at predetermined conclusions.
- DCIG did not guarantee any provider that its solution would be included in this TOP 5 report.
- DCIG did not imply or guarantee that a specific solution would receive a TOP 5 designation.
- All research is based upon publicly available information, information shared by the provider, and the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate how or if the features worked as described.
- No negative inferences should be made against any provider or solution not covered in this TOP 5 report.
- It is a misuse of this TOP 5 report to compare solutions included in this report against solutions not included in it.

2PB+ Cyber Secure Backup Targets // US Edition

No provider was privy to how DCIG weighted individual features. In every case the provider only found out the rankings of its solution after the analysis was complete. To arrive at the TOP 5 solutions included in this report, DCIG went through a seven-step process to come to the most objective conclusions possible.

1. DCIG established which features would be evaluated.
2. The features were grouped into five general categories.
3. DCIG weighted each feature to establish a scoring rubric.
4. DCIG identified solutions that met DCIG's definition for a 2PB+ cyber secure backup target.
5. A survey was completed for a model of each evaluated backup target.
6. DCIG evaluated each backup target based on information gathered in its survey.
7. Solutions were ranked using standard scoring techniques. ■

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of DCIG TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**